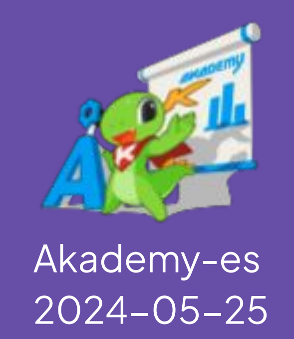
Cómo puedes utilizar OSS KB…

…para desarrollar en KDE



Akademy-es
2024–05–25

Agustín Benito Bethencourt
Miembro del Board de STF
abenito@kde-espana.es

Contenidos



1. – The speaker

Agustín Benito Bethencourt

@toscalix



Software Transparency Foundation

- Software Transparency Foundation (STF) Board member.
- Continuous Delivery, FLOSS, data analytics, agility and remote work advocate
- Independent consultant helping companies in two ways:
    - Applying advanced data analytics to production environments to increase delivery performance, partnering with Bitergia, through a service offering called Delivery Performance Analytics
    - Increasing their organizational performance by becoming good open source citizens, like in the case for SCANOSS, as their Ecosystem Manager
- Other activities
    - SwH Ambassador.
    - KDE e.V. member. KDE España founder member.
- More about Agustín
    - Background: MBition (Mercedes Benz), SUSE, Linaro, Eclipse Foundation, Codethink…
    - Blog - About - Talks

2. – Introduction

Software Composition Analysis (SCA)



Learn about Frankie: Frankie 1. Frankie 2

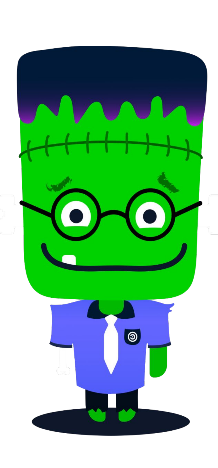
Software composition analysis (SCA) is an automated process that examines a codebase to identify all its components for various purposes:

- Detect dependencies (code management)
- Identify licenses (license compliance)
- Asses potential vulnerabilities (code quality)
- Identify crypto algorithms (export control)
- Security compliance, quantum safety, anti-plagiarism…

SCA market



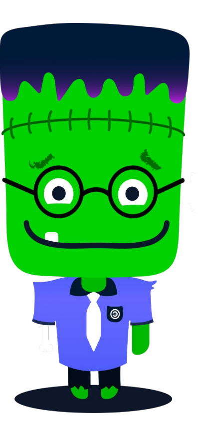
- SCA market started as a proprietary monopoly
- OSS grew but that monopoly remained
- Is it feasible to disrupt this market with:
  - OSS Business Model?
  - Open Data Business Model?
- SCANOSS challenges the status quo:
  - Open source software journey: every tool and component is OSS
  - Open data journey: OSS KB + open data sets



About SCANOSS



- Leaders: Alan Facey (CEO) and Julian Coccia (CTO)
- Registered in Madrid, ES. +30 staff.
- SCANOSS is an open source software company
  - Every software (developed or consumed) is OSS, including the APIs, algorithm implementations, plugins, tooling…
  - You can build your own KB and tools using SCANOSS software
  - Several open Source and proprietary tools use SCANOSS software today



- SCANOSS is a data company. IP: knowledge base (SCANOSS KB) of published-only OSS and mining network
- SCAN OSS is on an open data journey
  - OSS KB is a subset of SCANOSS KB. SCANOSS provided a perpetual license to STF to provide free (gratis) access to OSS KB
  - SCANOSS is publishing open dataset for various purposes: security, export control, etc.

Software Transparency Foundation (STF)



- Spanish foundation originally promoted by SCANOSS
- Mission: Solving Software Supply Chain Transparency
- STF provides confidential and free (gratis) access to OSS KB, guarantees a QoS so everyone can use it and provides a SBOM Ledger
- STF holds a perpetual license to host and provide access to OSSKB
- Support STF:
  - As non-profit: create a mirror and provide higher throughput for your members
  - As organization: sponsor STF to maintain/rise QoS for everyone and yourself
  - As individual: use and promote OSS KB
- Web. Linkedin



3. – OSS KB and Workbench

About OSS KB



- Open Source Software Knowledge Base is a subset of SCANOSS KB
- It is encrypted, maintained by SCANOSS for STF
- OSS KB is mostly focused on license compliance
- Accessible through STF or its mirrors via API
- The API to access OSS KB is OSS so
  - There are several implementations: .go, .js, .py
  - CLI and webhook available
  - You can use the API in your own tools like several tools do today, like FOSSology…

About Workbench



- sbom-workbench is an auditing GUI tool to complete your SCA:
    - file indexing and scanning
    - dependency scanning
    - vulnerability scanning
    - search indexing
- Workbench supplies information about your source code which includes reporting on the components and their corresponding dependencies, providing insights on licenses and incompatibilities.
- Workbench is *GPL-2.0-only* and uses OSS KB API by default

4. – It’s demo time!

Links and references



- Software Transparency Foundation: STF
- SCANOSS website. SCANOSS OSS at GitHub
- OSS KB. API
- Workbench
    - Workbench on GitHub
    - Latest stable release v.1.12.4. Download Workbench via Flathub (new)
- Videos
    - Tool Review: SCANOSS Audit Workbench
    - SCANOSS Python Tool

5.- Takeaway

Takeaway



You can’t protect or comply with what you cannot see

Takeaway



Curating software and creating SBOMs is a challenge for any developer

Takeaway



Software curation and SBOMs availability makes the consumption of your KDE software safer …

… especially in an AI-driven world

Takeaway



Workbench + OSS KB is a solid and affordable solution to this challenge for KDE developers

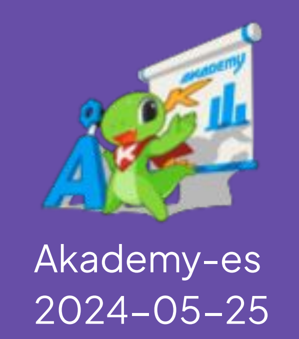
Thank you

Questions?



Cómo puedes utilizar OSS KB…

…para desarrollar en KDE



Akademy-es
2024-05-25

Agustín Benito Bethencourt
Miembro del Board de STF
abenito@kde-espana.es